KOENIG
step forward

Mastering Mastasploit Framework

Module 1 Introduction to Metasploit Framework

- Basic Terminologies
- Using Different Metasploit Interfaces
- Msfconsole
- Msfcli
- Msfvenom
- Msfencode
- *Lab Exercise*

Module 2 Information Gathering with Metasploit

- Penetration Testing Review
- Information Gathering
- Setting up Metasploit Database
- Port Scanning techniques
- Port Scanning with Nmap
- Nmap and Metasploit
- Metasploit Port Scanners
- *Lab Exercise*

Module 3 Vulnerability Scanning With Metasploit

- Vulnerability Scanning
- Vulnerability Scanning with Nessus
- Using Nessus from withing Metasploit
- Nmap Scripting Engine
- Metasploit Vulnerability Scanner
- Scanning Website for vulnerabilities
- Website scanning with Nikto
- *Lab Exercise*

Module 4 Exploitation With Metasploit

- Windows Exploitation

- Linux Exploitation
- Website Exploitation
- Exploiting Misconfigurations
- Metasploit Scripting
- Exploiting OS with Metasploit Scripting
- *Lab Exercise*

Module 5 Post Exploitation With Metasploit

- Working with Sessions
- Meterpreter
- Pivoting
- Meterpreter Scripts
- Enabling Remote Desktop
- Bypassing UAS
- *LAB Exercise*

Module 6 Advance Exploitation with Metasploit

- Client side Attacks
- Client Side Exploit
- Backdooring Binaries
- msfpayload
- Msfvenom
- Msfencode
- Social Engineering
- Social Engineering Toolkit
- Metasploit Browser Exploition Method
- Credential Harvester Attack Method
- Mass Mailer Attack
- *Lab Exercise*

Module 7 Exploit Development with Metasploit

- Essential terminologies
- Vulnerabilities in Freefloat FTP
- Pattern_create and Pattern_offset
- Hijacking Control
- Endianess

- Hijacking the CPU
- Buffer Overflow Exploit
- TFTP Fuzzer Module
- *Lab Exercise*

Module 8 Porting Exploit Into Metasploit

- Exploit Skeleton Overview
- Exploit Setting
- Exploit FTP Settings
- Definition of Exploit
- Testing the Exploit
- Configuring Exploit Options
- Exploit Module Review
- *Lab Exercise*